SYSTEMS AND METHODS FOR ENABLING A MOBILE USER TO NOTIFY AN AUTOMATED MONITORING SYSTEM OF AN EMERGENCY SITUATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U. S. Patent Application Serial No. 09/704,150, filed November 1, 2000, and entitled "System and Method for Monitoring and Controlling Residential Devices;" U.S. Patent Application Serial No. 09/271,517, filed March 18, 1999, and entitled "System For Monitoring Conditions in a Residential Living Community;" and U. S. Patent Application Serial No. 09/439,059, filed November 12, 1999, and entitled "System and Method for Monitoring and Controlling Remote Devices." Each of the identified U.S. Patent Applications is hereby incorporated by reference in its entirety. This application also claims the benefit of U.S. Provisional Application Serial No. 60/224,047, filed August 9, 2000, and entitled "Design Specifications for a Personal Security Device (FOB)," which is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

The present invention generally relates to remotely operated systems, and more particularly to a computerized system for monitoring and reporting on remote systems by transferring information via radio frequency (RF) signals via a message protocol system.

BACKGROUND

There are a variety of systems for monitoring and/or controlling any of a number of systems and/or processes, such as, for example, manufacturing processes, inventory systems, emergency control systems, personal security systems, residential systems, and electric utility meters to name a few. In many of these "automated monitoring systems," a host computer in communication with a communication network, such as a wide area network, monitors and/or controls a plurality of remote devices arranged within a geographical region. The plurality of remote devices typically use remote sensors and actuators to monitor and automatically respond to various system parameters to reach desired results. A number of automated monitoring

systems utilize computers to process sensor outputs, to model system responses, and to control actuators that implement process corrections within the system.

For example, both the electric power generation and metallurgical processing industries successfully control production processes by implementing computer control systems in individual plants. Home security has been greatly increased due to automated monitoring devices. Many environmental and safety systems require real-time monitoring. Heating, ventilation, and air-conditioning systems (HVAC), fire reporting and suppression systems, alarm systems, and access control systems utilize real-time monitoring and often require immediate feedback and control.

A problem with expanding the use of automated monitoring systems is the cost of the sensor/actuator infrastructure required to monitor and control such systems. The typical approach to implementing automated monitoring system technology includes installing a local network of hard-wired sensor(s)/actuator(s) and a site controller. There are expenses associated with developing and installing the appropriate sensor(s)/actuator(s) and connecting functional sensor(s)/actuator(s) with the site controller. Another prohibitive cost of control systems is the installation and operational expenses associated with the site controller.

Another problem with using automated monitoring system technology is the geographic size of automated monitoring systems. In a hard-wired automated monitoring system, the geographic size of the system may require large amounts of wiring. In a wireless automated monitoring system, the geographic size of the automated monitoring system may require wireless transmissions at unacceptable power levels.

Another problem is that communications within the automated monitoring system can only be initiated by the host computer, some other computing device connected to the host computer via a wide area network, or one of the remote devices being monitored. Individuals associated with the remote devices and/or personnel associated with the automated monitoring system have no additional means of communicating various conditions within the automated monitoring system. For example, in situations where the automated monitoring system is susceptible to emergency situations and/or unforeseen events, it may be beneficial to enable users and other personnel the ability to flexibly initiate communications without having to access the host computer.

Accordingly, there is a need for automated monitoring systems that overcome the shortcomings of the prior art.

SUMMARY OF THE INVENTION

The present invention provides systems and methods for enabling a mobile user to notify an automated monitoring system of an emergency situation. In general, the automated monitoring system may be configured for monitoring and controlling a plurality of remote devices and may comprise a site controller in communication with the plurality of remote devices via a plurality of transceivers defining a wireless communication network. The remote devices may be controlled via a host computer in communication with the site controller via a communication network, such as a wide area network.

The present invention may be viewed as providing a mobile communication device adapted for use with an automated monitoring system. The automated monitoring system may be configured for monitoring and controlling a plurality of remote devices and may comprise a site controller in communication with the plurality of remote devices via a plurality of transceivers defining a wireless communication network and in communication with a host computer via a wide area network. Briefly described, one of many possible embodiments of the mobile communication device comprises: memory, logic, and a wireless transmitter. Memory may comprise a unique identifier associated with the mobile communication device. The logic may be responsive to a transmit command and may be configured to retrieve the unique identifier from memory and generate a transmit message using a predefined communication protocol being implemented by the wireless communication network. The transmit message generated by the logic may comprise the unique identifier and may be configured such that the transmit message may be received by the site controller via the wireless communication network and such that the site controller may identify the mobile identification device and notify the host computer of the transmit message. The wireless transmitter may be configured for communication over the wireless communication network and configured to provide the transmit signal to the wireless communication network.

The present invention may also be viewed as providing a method for enabling a mobile user to notify an automated monitoring system of an emergency situation. Briefly described, one such method involves the steps of: receiving notification that the

mobile user desires to initiate transmission of an emergency message to the site controller; determining the identity of the mobile user; and providing an emergency message over the wireless communication network for delivery to the site controller, the emergency message indicating the identity of the mobile user.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings incorporated in and forming a part of the specification, illustrate several aspects of the present invention, and together with the description serve to explain the principles of the invention. In the drawings:

FIG. 1 is a block diagram illustrating one of a number of a number of possible embodiments of an automated monitoring system according to the present invention;

FIG. 2 is a block diagram illustrating one of a number of possible embodiment of the transceiver in FIG. 1 in communication with the sensor of FIG.1;

FIG. 3 is a high level diagram of one embodiment of a personnel communication device according to the present invention that may be used to communicate with the site controller of FIG. 1;

FIG. 4 is a block diagram of the architecture of the personnel communications device of FIG. 3;

FIG. 5 is a block diagram illustrating one of a number of possible embodiments of the site controller of FIG. 1;

FIG. 6 is a table illustrating the message structure of a communication protocol that may be implemented by the automated monitoring system of FIG. 1;

FIG. 7 is a table illustrating several exemplary values for the "to" address in the message structure of FIG. 6;

FIG. 8 illustrates three sample messages using the message protocol of the present invention; and

FIG. 9 illustrates another embodiment of the automated monitoring system according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Having summarized the invention above, reference is now made in detail to the description of the invention as illustrated in he drawings. While the invention will be described in connection with these drawings, there is no intent to limit it to the embodiment or embodiments disclosed therein. On the contrary, the intent is to cover

all alternatives, modifications and equivalents included within the spirit and scope of the invention as defined by the appended claims.

Reference is now made to FIG. 1, which is a schematic diagram illustrating an automated monitoring system 100 according to the present invention. The automated monitoring system 100 may comprise one or more applications servers 110 (one being shown for simplicity of illustration), one or more database servers 115, a WAN 120, one or more repeaters 125, one or more sensor/actuators 130, one or more transceivers 135, one or more sensors 140, one or more transmitters 145, and at least one site controller 150. As further illustrated in FIG. 1, each of the sensor/actuators 130 and the sensors 140 may be integrated with a suitably configured RF transceiver/repeater 125, an RF transceiver 135, or an RF transmitter 145. Hereinafter, the group including an RF transceiver/repeater 125, an RF transceiver 135, and an RF transmitter 145 will be referred to as RF communication devices.

The RF communication devices are preferably small in size and may be configured to transmit a relatively low-power RF signal. As a result, in some applications, the transmission range of a given RF communication device may be relatively limited. Of course, the transmitter power and range may be appropriately designed for the target operating environment. As will be appreciated from the description that follows, this relatively limited transmission range of the RF communications devices is advantageous and a desirable characteristic of the automated monitoring system 100. Although the RF communication devices are depicted without a user interface such as a keypad, *etc.*, in certain embodiments the RF communication devices may be configured with user selectable pushbuttons, switches, or an alphanumeric keypad suitably configured with software and or firmware to accept operator input. The RF communication device may be electrically interfaced with a sensor 140 or with a sensor/actuator 130, such as, for example, a smoke detector, a thermostat, a security system, *etc.*, where user selectable inputs may not be needed. It should be noted that the automated monitoring system 100 is being shown in FIG. 1 with a wide variety of components. One of ordinary skill in the art will appreciate that automated monitoring system 100 may include fewer or more components depending on design needs and the particular environment in which automated monitoring system is implemented.

As illustrated in FIG. 1, one or more sensors 140 may communicate with at least one site controller 150 via an RF transmitter 145, an RF transceiver 135, or an RF transceiver/repeater 125. Furthermore, one or more sensors/actuators 130 may be communicatively coupled to at least one site controller 150 via an RF transceiver 135 or an RF transceiver/repeater 125. In order to send a command from the applications server 110 to a sensor/actuator 130, the RF communication device in communication with the sensors/actuators 130 should be a two-way communication device (*i.e.*, a transceiver). One of ordinary skill in the art will appreciate that that one or more sensors/actuators 130 may be in direct communication with one or more site controllers 150. It will be further appreciated that the communication medium between the one or more sensor/actuators 130 and sensors 140 and the one or more site controllers 150 may be wireless or, for relatively closely located configurations, a wired communication medium may be used.

Alternatively, the RF transceiver 135 may be replaced by an RF transmitter 145. This simplifies the device structure, but also eliminates the possibility of the site controller 150 communicating with remote devices via the transmitter 145.

Automated monitoring system 100 may further comprise a plurality of stand-alone RF transceivers 125 acting as repeaters. Each repeater 125, as well as each RF transceiver 135, may be configured to receive one or more incoming RF transmissions (transmitted by a remote transmitter 145 or transceiver 135) and to transmit an outgoing signal. This outgoing signal may be another low-power RF transmission signal, a higher-power RF transmission signal, or alternatively may be transmitted over a conductive wire, fiber optic cable, or other transmission media. One of ordinary skill in the art will appreciate that, if an integrated RF communication device (*e.g.*, a RF transmitter 145, a RF transceiver 135, or a RF transceiver/repeater 125) is located sufficiently close to site controller 150 such that the RF signals may be received by the site controller 150, the data transmission signal need not be processed and repeated through either an RF transceiver/repeater 125 or an RF transceiver 135.

As illustrated in FIG. 1, one or more site controllers 150 may be configured and disposed to receive remote data transmissions from the various stand-alone RF transceiver/repeaters 125, integrated RF transmitters 145, and integrated RF transceivers 135. Site controllers 150 may be configured to analyze the transmissions received, convert the transmissions into TCP/IP format and further communicate the remote data signal transmissions to one or more applications servers 110 or other

computing devices connected to WAN 120. The site controller B 150 may function as either a back-up site controller in the event of a site controller failure or may function as a primary site controller to expand the potential size of the automated monitoring system 100. As a back-up site controller, the site controller B 150 may function when the applications server 110 detects a site controller failure. Alternatively, the site controller B 150 may function to expand the capacity of automated monitoring system 100. A single site controller 150 may accommodate a predetermined number of remote devices. While the number of remote devices may vary based upon individual requirements, in one embodiment, the number may be equal to approximately 500 remote devices. As stated above, additional site controllers 150 may increase the capacity of automated monitoring system 100. The number of RF communications devices that may be managed by a site controller 150 is limited only by technical constraints, such as memory, storage space, *etc.* In addition, the site controller 150 may manage more addresses than devices because some RF communications devices may have multiple functions, such as sensing, repeating, *etc.* Since the site controller 150 is in communication with WAN 120, applications server 110 may host application specific software. As described in more detail below, the site controller 150 may communicate information in the form of data and control signals to remote sensor/actuators 130 and remote sensors 140, which are received from applications server 110, laptop computer 155, workstation 160, *etc.* via WAN 120. The applications server 110 may be networked with a database 115 to record client specific data or to assist the applications server 110 in deciphering a particular data transmission from a particular sensor 140 or actuator/sensor 130.

One of ordinary skill in the art will appreciate that each RF communication device in automated monitoring system 100 has an associated antenna pattern (not shown). The RF communications devices are geographically disposed such that the antenna patterns overlap to create a coverage area 165, which defines the effective area of automated monitoring system 100.

As described in further detail below, automated monitoring system 100 may also include a mobile personal communication device (FOB) 170, which may transmit an emergency message directly or indirectly to a site controller 150. For example, in certain implementations of automated monitoring system 100, such as where the remote devices are electric utility meters or personal security systems, it may be beneficial to enable FOB 170 to transmit an emergency message configured to notify the site

controller 150 of the occurrence of an emergency situation. In this manner, automated monitoring system 100 may an FOB 170 configured to transmit an electromagnetic signal that may be encoded with an identifier that is unique to the FOB 170.

Reference is now made to FIG. 2, which is a block diagram illustrating one embodiment of the transceiver 135 and sensor 130 of FIG. 1 in communication with each other. Sensor 130 may be any type of device configured to sense one or more parameters. For example, sensor 130 may be a two-state device such as a smoke alarm. Alternatively, sensor 130 may output a continuous range of values, such as the current temperature, to transceiver 135. If the signal output from the sensor 130 is an analog signal, data interface 205 may include an analog-to-digital converter (not shown) to convert signals provided to the transceiver 135. Alternatively, where sensor 130 provides digital signals, a digital interface may be provided.

In FIG. 2, the sensor 130 may be communicatively coupled with the RF transceiver 135. The RF transceiver 135 may comprise a transceiver controller 210, a data interface 205, a data controller 215, memory 220, and an antenna 225. As shown in FIG. 2, a data signal provided by the sensor 130 may be received at the data interface 205. In situations where the data interface 205 has received an analog data signal, the data interface 205 may be configured to convert the analog signal into a digital signal before forwarding a digital representation of the data signal to the data controller 215.

The RF transceiver 135 has a memory 220 that may contain a unique transceiver identifier that uniquely identifies the RF transceiver 135. The transceiver identifier may be programmable and implemented in the form of, for example, an EPROM. Alternatively, the transceiver identifier may be set/configured through a series of dual inline package (DIP) switches. One of ordinary skill in the art will appreciate that the transceiver identifier and memory 220 may be implemented in a variety of additional ways.

While the unique transceiver address may be varied in accordance with the present invention, it preferably may be a six-byte address. The length of the address may be varied as necessary given design needs. Using the unique transceiver address, the RF communication devices and the site controller 150 may determine, by analyzing the data packets, which devices generated and/or repeated the data packet.

Of course, additional and/or alternative configurations may also be provided by a similarly configured transceiver. For example, a similar configuration may be provided for a transceiver that is integrated into, for example, a carbon monoxide detector, a door position sensor, etc. Alternatively, system parameters that vary across a range of values may be transmitted by transceiver 135 as long as data interface 205 and data controller 215 are configured to apply a specific code that is consistent with the input from sensor 130. As long as the code is understood by the applications server 110 (FIG. 1) or workstation 160 (FIG. 1), the target parameter may be monitored.

FIG. 3 shows a high level diagram of the interaction of the personnel communication device (FOB) 170 and the site controller 150 according to the present invention. The FOB 170 communicates directly or indirectly with the site controller 150. While the FOB 170 will be described in more detail below, in general the FOB 170 transmits an electromagnetic signal to a site controller 150 and/or an RF communication device. The electromagnetic signal may be encoded with a unique transceiver identifier associated with the FOB 170. An internal circuit (not shown) may be provided within the FOB 170 to act upon command to transmit the encoded electromagnetic signal 320. A transmit button 325 may be provided for the user. In the embodiment illustrated in FIG. 3, the FOB 170 is quite small and may be conveniently attached, for example, to a key ring 330, clothing (not shown), *etc.* for ready and portable use. Furthermore, FOB 170 may be integrated with a mobile electronics device. For instance, FOB 170 may be integrated with a handheld computer, such as a personal digital assistant (PDA), a wireless telephone, or any other mobile electronics device.

Indeed, in another embodiment, the single FOB 170 may serve multiple functions. For example, an FOB 170 may be integrally designed with another device, such as an automotive remote, to provide the dual functionality of remotely controlling an automobile alarm along with the functionality of the FOB 170. In accordance with such an embodiment, a second transmit button 335 may be provided. The first transmit button 325 may be operative to, for example, communicate with the site controller 150, while the second transmit button 335 may be operative to remotely operate the automobile alarm. One of ordinary skill in the art will appreciate that FOB 170 may be integrated with any of a variety of alternative devices with one or more transmit buttons 335. Furthermore, it will be appreciated that the frequency and/or format of the

transmit signal 320 transmitted may be different for the different applications. For example, the FOB 170 may transmit a unique identifier to the site controller 150 (FIG. 1), while only a unique activation sequence need be transmitted to actuate an automobile alarm or other device.

In use, a user may simply depress transmit button 325, which would result in the FOB 170 transmitting an electromagnetic signal 320 to the site controller 150. Preferably, the FOB 170 is low power transmitter so that a user may only need to be in close proximity (*e.g.*, several feet) to site controller 150 or one of the RF communication devices of the automated monitoring system 100 (FIG. 1). The FOB 170 may communicate either directly with the site controller 150, if in close proximity, or indirectly via the transceivers and/or repeaters of the automated monitoring system 100. Low-power operation may help to prevent interception of the electromagnetic signals. In alternative embodiments, FOB 170 may be configured such that the transmitted signal may be encrypted for further protect against interception.

The site controller 150 receives and decodes the signal 320 via RF transceiver 340. The site controller 150 then evaluates the received, decoded signal to ensure that the signal identifies a legitimate user. If so, the site controller 150 sends an emergency message to the applications server 110 (FIG. 1).

Having now presented an overview of the basic operation of FOB 170, reference is made to FIG. 4 which shows a more detailed block diagram of the components contained within an embodiment of FOB 170. As previously mentioned, the FOB 170 includes a transmit button 325, which initiates the data transmission. FOB 170 may include a memory 405, a data formatter 410, a controller 415, and an RF transmitter 420. Depending upon the desired complexity of the automated monitoring system 100 and FOB 170, the RF transmitter 420 may be replaced by an RF transceiver.

Controller 415 controls the overall functionality of FOB 170. The controller 415 is responsive to the depression or actuation of transmit button 325 to begin the data transaction and signal transfer. When a user depresses the transmit button 325, the controller 415 initiates the data transmission sequence by accessing the memory 405, which, among other things, stores the transceiver unique identifier. This information is then passed to the data formatter 410, which places the data in an appropriate and predefined format for transmission to the site controller 150. One of ordinary skill in the art will appreciate that the data may be retrieved from memory 405

and translated into the predefined format as electronic data or in a variety of other ways. When electronic data is used, the data is sent from data formatter 410 to RF transmitter 420 for conversion from electronic to electromagnetic form. As well known by those skilled in the art, a variety of transducers may perform this functionality. One of ordinary skill in the art will appreciate that FOB 170 may implement any of a variety of communication protocols and data formats for communication with automated monitoring system 100. In one embodiment, FOB 170 may implement the communication protocol used by automated monitoring system 100, which is described in more detail below with respect to FIGS. 6 – 8.

It will be appreciated by persons skilled in the art that the various RF communication devices may be configured with a number of optional power supply configurations. For example, the FOB 170 (FIG. 4) may be powered by a replaceable battery. Those skilled in the art will appreciate how to meet the power requirements of the various devices. As a result, it is not necessary to further describe a power supply suitable for each device and each application in order to appreciate the concepts and teachings of the present invention.

Having illustrated and described the operation of the various combinations of RF communication devices with the various sensors 140, reference is now made to FIG. 5, which is a block diagram further illustrating one embodiment of a site controller 150. According to the present invention, a site controller 150 may comprise an antenna 510, a transceiver controller 515, a central processing unit (CPU) 520, memory 525, a network card 530, a digital subscriber line (DSL) modem 535, an integrated services digital network (ISDN) interface card 540, as well as other components not illustrated in FIG. 5, capable of enabling a transfer control protocol / Internet protocol (TCP/IP) connection to WAN 120.

The transceiver controller 515 may be configured to receive incoming RF signal transmissions via the antenna 510. Each of the incoming RF signal transmissions are consistently formatted as described below. Site controller 150 may be configured such that the memory 525 includes a look-up table 545 configured for identifying the various wireless communication devices (including intermediate wireless communication devices) used in generating and transmitting the received data transmission. As illustrated in FIG. 5, site controller 150 may include an "Identify Remote Transceiver" memory sector 550 and an "Identify Intermediate Transceiver" memory sector 555. Programmed or recognized codes within the memory 525 may also be provided and

configured for controlling the operation of a CPU 520 to carry out the various functions that are orchestrated and/or controlled by the site controller 150. For example, the memory 525 may include program code for controlling the operation of the CPU 520 to evaluate an incoming data packet to determine what action needs to be taken. In this regard, one or more look-up tables 545 may also be stored within the memory 525 to assist in this process. Furthermore, the memory 525 may be configured with program code configured to identify a remote RF transceiver 550 or identify an intermediate RF transceiver 555. Function codes, RF transmitter, and/or RF transceiver identification numbers may all be stored with associated information within the look-up tables 545.

Thus, one look-up table 545 may be provided to associate transceiver identificatiers with a particular user. Another look-up table 545 may be used to associate function codes with the interpretation thereof. For example, a first data packet segment 550 may be provided to access a first lookup table to determine the identity of the RF transceiver (not shown) that transmitted the received message. A second code segment may be provided to access a second lookup table to determine the proximate location of the RF transceiver that generated the message by identifying the RF transceiver that relayed the message. A third code segment may be provided to identify the content of the message transmitted. Namely, is it a fire alarm, a security alarm, an emergency request by a person, a temperature control setting, *etc.* In accordance with the present invention, additional, fewer, or different code segments may be provided to carry out different functional operations and data signal transfers of the present invention.

The site controllers 150 may also include one or more network interface devices configured for communication with WAN 120. For example, the site controller 150 may include a network card 530, which may allow the site controller 150 to communicate across a local area network to a network server, which in turn may contain a backup site controller (not shown) to the WAN 120. Alternatively, the site controller 150 may contain a DSL modem 535, which may be configured to provide a link to a remote computing system via the public switched telephone network (PSTN). The site controller 150 may also include an ISDN card 540 configured to communicate via an ISDN connection with a remote system. Other communication interfaces may be provided to serve as primary and/or backup links to the WAN 120 or to local area networks that might serve to permit local monitoring of the operability of site controller 150 and to permit data packet control.

Automated monitoring system 100 may implement any of a variety of types of message protocols to facilitate communication between the remote devices, the RF transceivers, and the site controller 150. FIG. 6 sets forth a message structure for implementing a data packet protocol according to the present invention. All messages transmitted within the automated monitoring system 100 may consist of a "to" address 600, a "from" address 610, a packet number 620, a number of packets in a transmission 630, a packet length 640, a message number 650, a command number 660, any data 670, and a check sum error detector (CKH 680 and CKL 690).

The "to" address 600 indicates the intended recipient of the packet. This address can be scalable from one to six bytes based upon the size and complexity of automated monitoring system 100. By way of example, the "to" address 600 may indicate a general message to all transceivers, to only the stand-alone transceivers, or to an individual integrated transceiver. In a six byte "to" address, the first byte may indicate the transceiver type – to all transceivers, to some transceivers, or a specific transceiver. The second byte may be the identification base, and bytes three through six may be used for the unique transceiver address (either stand-alone or integrated). The "to" address 600 may be scalable from one byte to six bytes or larger depending upon the intended recipient(s).

The "from" address 610 may be a six-byte unique transceiver address of the transceiver originating the transmission. The "from" address 610 may be the address of the site controller 150 when the controller requests data, or this can be the address of the integrated transceiver when the integrated transceiver sends a response to a request for information to the site controller 150.

The packet number 620, the packet maximum 630, and the packet length 640 may be used to concatenate messages that are greater than 128 bytes. The packet maximum 630 may indicate the number of packets in the message. The packet number 620 may be used to indicate a packet sequence number for multiple-packet messages.

The message number 650 may be assigned by the site controller 150. Messages originating from the site controller 150 may be assigned an even number. Responses to the site controller 150 may have a message number 650 equal to the original message number 650 plus one, thereby rendering the responding message number odd. The site controller 150 then increments the message number 650 by two for each new

originating message. This enables the site controller 150 to coordinate the incoming responses to the appropriate command message.

The next section is the command byte 660 that may be used to request data from the receiving device as necessary. One of ordinary skill in the art will appreciate that, depending on the specific implementation of automated monitoring system 100, the types of commands may differ. In one embodiment, there may be two types of commands: device specific and not device specific. Device specific commands control a specific device such as a data request or a change in current actuator settings. Commands that are not device specific may include, but are not limited to, a ping, an acknowledge, a non-acknowledgement, downstream repeat, upstream repeat, read status, emergency message, and a request for general data among others. General data may include a software version number, the number of power failures, the number of resets, *etc.*

The data section 670 may contain data as requested by a specific command. The requested data may be any value. By way of example, test data may be encoded in ASCII (American Standard Code for Information Interchange) or other known encoding systems as known in the art. The data section 670 of a single packet may be scalable, for example, up to 109 bytes. In such instances, when the requested data exceeds 109 bytes, the integrated transceiver may divide the data into an appropriate number of sections and concatenate the series of packets for one message using the packet identifiers as discussed above.

Checksum sections 680 and 690 may used to detect errors in the transmissions of the packets. In one embodiment, errors may be detected using cyclic redundancy check sum methodology. This methodology divides the message as a large binary number by the generating polynomial (in this case, CRC-16). The remainder of this division is then sent with the message as the checksum. The receiver then calculates a checksum using the same methodology and compares the two checksums. If the checksums do not match, the packet or message will be ignored. While this error detection methodology is preferred, one of ordinary skill in the art will appreciate that other error detection systems may be employed.

One of ordinary skill in the art will appreciate that automated monitoring system 100 may employ wireless and/or wired communication technologies for communication between site controller 150 and the RF transceivers. In one embodiment, communication between site controller 150 and the RF transceivers may

be implemented via an RF link at a basic rate of 4,800 bits per second (bps) and a data rate of 2400 bps. All the data may be encoded in Manchester format such that a high to low transition at the bit center point represents a logic zero and a low to high transition represents a logic one. One of ordinary skill in the art will appreciate that other RF formats may be used depending upon design needs. By way of example, a quadature phase shift encoding method may also be used, thereby enabling automated monitoring system 100 to communicate via hexadecimal instead of binary.

Messages may further include a preface and a postscript (not shown). The preface and postscripts are not part of the message body but rather serve to synchronize automated monitoring system 100 and to frame each packet of the message. The packet may begin with the preface and end with a postscript. The preface may be a series of twenty-four logic ones followed by two bit times of high voltage with no transition. The first byte of the packet may then follow immediately. The postscript may be a transition of the transmit data line from a high voltage to a low voltage. It may be less desirable to not leave the transmit data line high after the message is sent. Furthermore, one of ordinary skill in the art will appreciate that the preface and the postscript may be modified as necessary for design needs.

FIG. 7 sets forth one embodiment of the "to" address byte assignment. The "to" address may take many forms depending on the specific requirements of automated monitoring system 100. In one embodiment, the "to" address may consist of six bytes. The first byte (Byte 1) may indicate the device type. The second byte (Byte 2) may indicate the manufacturer or the owner. The third byte (Byte 3) may be a further indication of the manufacturer or owner. The fourth byte (Byte 4) may indicate that the message is for all devices or that the message is for a particular device. If the message is for all devices, the fourth byte may be a particular code. If the message is for a particular device, the fourth, fifth, and sixth bytes (Byte 5 and Byte 6) may include the unique identifier for that particular device.

Having described the general message structure of the present invention, reference is directed to FIG. 8. FIG. 8 illustrates the general message structure for an emergency message. The message illustrates the broadcast of an emergency message "FF" from a central server with an address "001234567" to a integrated transceiver with an address of "FF."

Returning to FIG. 1, the site controller 150 functions as the local communications master in automated monitoring system 100. With the exception of emergency messages, the site controller 150 may initiate communication with any RF communication device. The RF communication device then responds based upon the command received in the message. In general, the site controller 150 may expect a response to all messages sent to any of the RF communication devices. By maintaining the site controller 150 as the communications master and storing the collected data at the site controller 150, overall system installation, upkeep costs, and expansion costs may be minimized. By simplifying the RF communication devices, the initial cost and maintenance of the RF communication devices may be minimized. Further information regarding the normal mode of communications can be found in U. S. Patent Application Serial No. 09/812,044, entitled "System and Method for Monitoring and Controlling Remote Devices," and filed March 19, 2001, which is hereby incorporated in its entirety by reference.

As stated above, automated monitoring system 100 may be configured such that other devices, such as FOB 170 and certain RF transceivers, may initiate emergency messages. To accommodate receiving emergency messages, the site controller 150 may dedicate a predetermined time period, for example one-half of every ten-second period, to receive emergency messages. During these time periods, the site controller 150 may not transmit messages other than acknowledgements to any emergency messages. The integrated transceiver 135 may detect the period of silence, and in response, may then transmit the emergency message.

There are typically two forms of emergency messages: from the FOB 170 and from permanently installed safety/security transceiver(s). In the first case of the FOB 170, the emergency message may comprise a predetermined "to" address and a random odd number. In response to this emergency message, the site controller 150 may acknowledge during a silent period. The FOB 170 then repeats the same emergency message. The site controller 150 may forward the emergency message to the WAN 120 in the normal manner.

Upon receipt of the site controller 150 acknowledgement, the FOB 170 may reset itself. If no acknowledgement is received within a predetermined time period, the FOB 170 may continue to re-transmit the original emergency message until acknowledged by the site controller 150 for a predetermined number of re-transmissions.

One of ordinary skill in the art will appreciate that the RF transceivers of the present invention may be further integrated with a voice-band transceiver. As a result, when a person presses, for example, the emergency button on his/her FOB 170, medical personnel, staff members, or others may respond by communicating via two-way radio with the party in distress. In this regard, each transceiver may be equipped with a microphone and a speaker that would allow a person to communication information such as their present emergency situation, their specific location, *etc.*

FIG. 9 sets forth another embodiment of automated monitoring system 100 according to the present invention. FIG. 9 illustrates the automated monitoring system 100 of FIG. 1 with an additional sensor 180 and transceiver 185. The additional sensor 180 and transceiver 185 may communicate with, but outside of, the coverage area 165 of the automated monitoring system 100. In this example, the additional sensor/transceiver may be placed outside of the original coverage area 165. In order to communicate , the coverage area of transceiver 185 need only overlap the coverage area 165. By way of example only, the original installation may be a system that monitors electricity via the utility meters in an apartment complex. Later a neighbor in a single family residence nearby the apartment complex may remotely monitor and control their thermostat by installing a sensor/actuator transceiver according to the present invention. The transceiver 185 then communicates with the site controller 150 of the apartment complex. If necessary, repeaters (not shown) may also be installed to communicate between the neighboring transceiver 185 and the apartment complex site controller 150. Without having the cost of the site controller, the neighbor may enjoy the benefits of automated monitoring control system 100.

The foregoing description has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the inventions to the precise embodiments disclosed. Obvious modifications or variations are possible in light of the above teachings. When the transceiver is permanently integrated into an alarm sensor or other stationary device within a system, then the application server 110 and/or the site controller 150 may be configured to identify the transceiver location by the transceiver identification number alone. It will be appreciated that, in embodiments that do not utilize stand-alone transceivers, the transceivers may be configured to transmit at a higher RF power level in order to effectively communicate with the control system site controllers.

It will be appreciated by those skilled in the art that the information transmitted and received by the wireless transceivers of the present invention may be further integrated with other data transmission protocols for transmission across telecommunications and computer networks. In addition, it should be further appreciated that telecommunications and computer networks may function as the transmission path between the networked wireless transceivers, the site controllers 150, and the applications servers 110.